UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/577,660	05/01/2006	**Richard Middleton Hicks**	9664-0003	8461

73552 7590 06/15/2011

Stolowitz Ford Cowger LLP
621 SW Morrison St
Suite 600
Portland, OR 97205

EXAMINER	
CALLAHAN, PAUL E	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
06/15/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/577,660	HICKS, RICHARD MIDDLETON	
	Examiner	Art Unit	
	PAUL CALLAHAN	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 May 2011*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-6,8-12,14-20,22,24-28,30-34,36,37 and 39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-6,8-12,14-16,18-20,22,24-26,28,30-34,36,37 and 39* is/are rejected.

7)☒ Claim(s) *17 and 27* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is prompted by the Applicant's response filed 5-12-2011.

2. Claims 1, 2, 4-6, 8-12, 14-20, 22, 24-28, 30-34, 36, 37 and 39 are pending and have been examined.

Response to Arguments

3. Applicant's arguments with respect to the claims have been considered and are persuasive. The Benoit reference has been withdrawn and new rejections using new art: Feigen et al., US 2002/0138554, have been written.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 2, 5, 6, 8-12, 14-16, 18-20, 22, 24-26, 28, 30-34, 36, 37, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cowie et al. US 2003/0023865 A1, Feigen et al., US 2002/0138554, and Pierre Richer: SANS/GIAC Practical Assignment for GSEC Certification Version 1.4b: Steganalysis: Detecting

hidden information with computer forensic analysis, SANS Institute 2003 (Submitted with the Applicant's IDS).

As for claims 1 and 39, Cowie teaches a method, comprising, obtaining a signature by reading code comprising a partial section of a program, (fig. 5: element 18, [0015], [0034], [0048]) comparing the signature with one or more computer files (fig. 5: element 18, [0015], [0034], [0048]), and, displaying a listing of which of the one or more computer-files provide a match with the signature (fig. 6 element 46, [0050]). Cowie does not teach that the code read is executable code or that partial sections of the software code are read. However Feigen does teach these features ([0009], [0010]: a hash signature of a block of code where the block is a portion of a larger executable [0014]) Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate this feature into the system of Cowie. It would have been obvious to do so since this would increase the probability of detecting hidden malware code in a file. Cowie fails to teach the feature where the computer-program is a steganographic program that includes software calls. However Richer does teach such a feature (page 4: Tools Used to Hide Information, page 6: Detecting Hidden Information With Various Resources: 1.) Guidance Software Inc. where comparisons of an original file MD5 hash is made with a MD5 hash of a suspect file in order to detect steganographically embedded data). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate this feature into the system of Cowie. It would have been obvious to do so

since this would extend the types of programs that can be evaluated for embedded malware detectable via the comparison step of Cowie.

As for claim 2, Cowie teaches a method according to claim 1 wherein the indication incorporates an identification of the item's location in the computer system ([0048]-[0050]).

As for claim 5, Cowie teaches a method according to claim 1, where an asserted file type is ignored when comparing files with the signature ([0048], [0050]: non WIN32 PE files excluded).

As for claim 6, Cowie teaches a method according to claim 1 wherein the step of comparing the signature with files is for each file preceded by checking the respective real file type by reading the start of the file and excluding computer files having prearranged initial byte sequences from comparing with the signature (fig. 6 element 32, [0049]: initial byte sequence is used to determine if file is a WIN32 PE file and if not, exclude it from further processing).

As for claims 8, 18, and 28, each of these claims is directed to the case where the file is a deleted or logical wastebasket file. Cowie teaches this feature ([0030]: WIN32 PE file type includes such files).

As for claim 9, Cowie teaches a method according to claim 1 wherein the one or more computer files comprise self-extracting executable files ([0006]).

As for claim 10, Cowie teaches a method according to claim 1 wherein some prearranged files are not identified in the listing despite containing software code which matches a signature ([0050]).

As for claims 11, the claim is directed towards the apparatus carrying out the method of claims 1. Claim 11 recites substantially the same limitations as claims 1 and therefore is rejected on the same basis as that claim.

As for claim 12, Cowie teaches a method according to claim 1 wherein the indication incorporates an identification of the matching signature ([0048]-[0050]).

As for claim 14, Cowie teaches the apparatus according to claim 11 where the code of the signature comprises a continuous sequence of the partial section of the program code (fig. 5: element 18, [0015], [0034], [0048]).

Claim 15 represents the apparatus carrying out the method steps of claim 5. Claim 15 recites substantially the same limitation as claim 5 and is therefore rejected on the same basis as that claim.

As for claim 16, Cowie teaches the apparatus of claim 11 wherein the partial section of code comprises a start of the computer file, and wherein computer files having a prearranges initial byte sequence are excluded for comparison (fig. 6 element 32, [0030]: file header is examined to determine if the file is a WIN32 PE file, a byte sequence is inherent for any such sequence of digital data).

As for claim 19, Cowie teaches the apparatus according to claim 11 wherein the one or more files comprise polymorphic files (fig. 5 element 16, [0048]: Trojan containing files include polymorphic malware).

As for claim 20, Cowie teaches the apparatus according to claim 11 wherein one or more predetermined files are not indicated despite containing code which matches a signature ([0048], [0050]: non WIN32 PE files excluded).

As for claim 22, Cowie teaches the computer-program product of claim 11 further comprising identifying a steganographic item responsible for the match ([0048] - [0050]: Trojan signature).

As for claim 24, Cowie teaches the computer-program product of claim 11, wherein the signature comprises a continuous sequence of program code but not more than 5% or less than 0.167% of the program (fig. 5: element 18, [0015], [0034], [0048]: header data is used for the signature).

As for claim 25, Cowie teaches the computer-program product of claim 31 wherein an asserted file type is not compared with the signature ([0048], [0050]: non WIN32 PE files excluded).

As for claim 26, this claim is directed towards the computer-program product that directs a processor to carry out the method of claim 16. Claim 26 recites substantially the same limitations as claim 16 and is therefore rejected on the same basis as that claim.

As for claim 30, this claim is directed towards the computer-program product that directs a processor to carry out the method of claim10. Claim 30 recites substantially the same limitations as claim 10 and is therefore rejected on the same basis as that claim.

As for claim 31, the claim is directed towards a computer program product that directs a processor to carry out the method of claim 1. Claim 31 recites substantially the same limitations as claims 1 and is therefore is rejected on the same basis as that claim.

As for claim 32, Cowie teaches the computer-readable medium of claim 31, wherein the method further comprises executing the one or more files, and wherein the

comparison is made prior to executing the one or more files ([0030]-[0031]: identification of banned game programs prior to being run on a business computer).

As for claim 33, Cowie teaches the method of claim 1, further comprising running a virus checking program while comparing the signature with one or more computer files (fig. 5: element 18, [0015], [0034], [0048]: the signature comparison algorithm of Cowie is an anti-viral program).

As for claim 34, Cowie teaches the apparatus according to claim 15, wherein the one or more predetermined file types are a graphics editor ([0030]: WIN32 PE file type includes graphics editors).

As for claim 36, Cowie teaches the computer apparatus according to claim 11, wherein the apparatus is further configured to analyze the one or more test signatures with a virus checking program in combination with the comparison with the steganographic signature (fig. 5, fig. 6, [0049], [0049]).

As for claim 37, the claim is directed towards the computer readable medium that directs a processor to carry out the method of claim 11. Claim 37 recites substantially the same limitations as claim 11 and is rejected on the same basis as that claim.

5. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cowie,

Atkinson and Richer as applied to claim 1 above, and further in view of Charbonneau, US 7,526,654.

As for claim 4, the combination of Cowie, Atkinson and Richer teaches the method according to claim 1, but not explicitly wherein the code that is read is a .DDL file. However, Charbonneau does teach such a feature (col. 5 lines 10-20). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate this feature into the system of Cowie and Richer. It would have been obvious to do so since this would extend the types of files where embedded malware is detectable via the comparison step of Cowie.

Allowable Subject Matter

6. Claims 17 and 27 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Eleni Shiferaw, can be reached on (571) 272-3867. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/PEC/
AU2437

/Eleni A Shiferaw/

Supervisory Patent Examiner, Art Unit 2437